Guía de Desktop Management

Ordenadores de escritorio para empresas

Número de referencia del documento: 312947-072

Septiembre de 2003

Esta guía ofrece definiciones e instrucciones sobre cómo utilizar las funciones de seguridad e Intelligent Manageability ya preinstaladas en algunos modelos.

Hewlett-Packard Company no se hace responsable de las omisiones ni de los errores técnicos o de edición que pueda contener este documento ni de los daños, fortuitos o consecuentes, relacionados con la instalación, rendimiento o uso de este material. La información contenida en este documento se proporciona "como está", sin garantía de ningún tipo, incluyendo pero sin limitarse a, las garantías implícitas de comerciabilidad e idoneidad para un propósito determinado y está sujeta a modificaciones sin previo aviso. Las garantías para los productos de HP están estipuladas en las declaraciones expresas de garantía limitada que acompañan a dichos productos. La información contenida en este documento no debe interpretarse como una garantía adicional.

ADVERTENCIA: cuando el texto aparece de este modo significa que, si no se siguen las instrucciones, pueden producirse lesiones físicas e incluso la muerte.

PRECAUCIÓN: cuando el texto aparece de este modo significa que, si no se siguen las indicaciones, se puede dañar el equipo o perder información.

Guía de Desktop Management
Ordenadores de escritorio para empresas

Segunda edición (Septiembre de 2003)
Número de referencia del documento: 312947-072

Contenido

Guía de Desktop Management

Índice

Guía de Desktop Management

Intelligent Manageability de HP proporciona soluciones basadas en estándares para gestionar y controlar equipos de sobremesa, workstations y ordenadores portátiles en un entorno de red. HP fue pionera en la manejabilidad de equipos de sobremesa con la introducción en 1995 de los primeros equipos personales de sobremesa completamente manejables de la industria. HP tiene una patente en tecnología de manejabilidad. Desde entonces, HP ha realizado grandes esfuerzos para desarrollar los estándares y la infraestructura necesarios para distribuir, configurar y gestionar de forma efectiva equipos de sobremesa, workstations y ordenadores portátiles. HP trabaja en estrecha colaboración con los proveedores de soluciones de software de gestión líderes en la industria para garantizar la compatibilidad entre Intelligent Manageability y estos productos. Intelligent Manageability supone un aspecto importante de nuestro compromiso general de proporcionar soluciones para PC que le ayuden durante las cuatro fases de éste: planificación, distribución, gestión y transición.

Las capacidades y funciones clave en la gestión de equipos de sobremesa son:

- Configuración y distribución inicial
- Instalación remota del sistema
- Actualización y gestión del software
- Memoria flash de la ROM
- Seguridad y seguimiento de activos
- Recuperación y notificación de fallos

Las funciones específicas admitidas que se describen en esta guía varían según el modelo o la versión de software.

Configuración y distribución inicial

El equipo se entrega con una imagen de software del sistema preinstalada. Después de un breve proceso de "desempaquetado" del software, el equipo está listo para ser utilizado.

Si lo desea, puede sustituir la imagen de software preinstalada por un conjunto personalizado de software del sistema y aplicaciones. Una imagen de software personalizada puede distribuirse de varias formas. Por ejemplo:

- Instalar aplicaciones de software adicionales tras desempaquetar la imagen de software preinstalada.
- Utilizar herramientas de distribución de software como Altiris Deployment Solution™, para sustituir el software preinstalado por una imagen de software personalizada.
- Mediante un proceso de clonación del disco para copiar el contenido de una unidad de disco duro a otra.

El mejor método de distribución depende de los procesos y del entorno de TI. En la sección sobre la distribución del PC (PC Deployement) de la página Web HP Lifecycle Solutions (Soluciones para el ciclo de vida de HP) en http://h18000.www1.hp.com/solutions/pcsolutions, se proporciona información sobre cómo seleccionar el mejor método de distribución.

El CD *Restore Plus!*, la configuración basada en la memoria ROM y el hardware ACPI proporcionan más ayuda en la recuperación del software del sistema, la gestión y solución de problemas de configuración, y la gestión de energía.

Instalación remota del sistema

La función Instalación remota del sistema (Remote System Installation) sirve para iniciar y configurar el sistema mediante la información de software y configuración localizada en un servidor de red mediante la inicialización del Entorno de ejecución previa al arranque (PXE del inglés Preboot Execution Environment). Esta función se utiliza generalmente como una herramienta de configuración del sistema y puede utilizarse en las tareas siguientes:

- Dar formato a una unidad de disco duro
- Distribuir una imagen de software en uno o más PC nuevos

- Actualizar de forma remota el BIOS del sistema en la memoria flash de la ROM ("Memoria flash de la ROM remota" en la página 7)
- Configurar los parámetros del BIOS del sistema

Para iniciar la instalación remota del sistema, pulse **F12** cuando aparezca el mensaje F12 = Network Service Boot (F12 = Arranque de servicio en red) en la esquina inferior derecha de la pantalla del logotipo de HP. Siga las instrucciones que aparecen en la pantalla para continuar con el proceso. El orden de arranque predeterminado es un parámetro de la configuración del BIOS que se puede modificar para intentar arrancar siempre mediante PXE.

HP y Altiris, Inc. se han asociado con el fin de proporcionar herramientas diseñadas para facilitar la tarea de distribución y gestión del PC corporativo y reducir el tiempo invertido en ella, y en última instancia, para reducir el coste total de propiedad y hacer de los PC de HP los PC cliente más manejables en el entorno de empresa.

Actualización y gestión del software

HP proporciona varias herramientas para gestionar y actualizar el software de los equipos de sobremesa y workstations, como por ejemplo, Altiris; Altiris PC Transplant Pro; HP Client Manager Software, una solución Altiris; System Software Manager; Proactive Change Notification y ActiveUpdate.

HP Client Manager Software

El software inteligente HP Client Manager Software (HP CMS) integra la tecnología Intelligent Manageability de HP dentro de Altiris para proporcionar unas capacidades superiores de gestión de hardware para dispositivos de acceso de HP, como por ejemplo:

- Vistas detalladas de inventario de hardware para la gestión de activos
- Diagnóstico y supervisión del funcionamiento del PC
- Notificación proactiva de cambios en el entorno de hardware
- Informes accesibles vía Internet sobre detalles críticos de la empresa, como máquinas con advertencias térmicas, alertas de memoria, etc

- Actualización remota del software del sistema, como por ejemplo, controladores de dispositivo y ROM BIOS
- Modificación remota del orden de arranque

Para obtener más información sobre HP Client Manager, visite http://h18000.www1.hp.com/im/client_mgr.html.

Soluciones Altiris

HP Client Management Solutions proporciona una gestión del hardware centralizada de los dispositivos cliente de HP en todas las áreas del ciclo de vida informático.

- Inventario y gestión de activos
  - ❏ Cumplimiento de la licencia del software
  - ❏ Informes y seguimiento del PC
  - ❏ Contrato de arrendamiento, seguimiento de activos
- Distribución y migración
  - ❏ Migración a Microsoft Windows 2000, Windows XP Professional o Home Edition
  - ❏ Distribución del sistema
  - ❏ Migraciones de personalidad
- Help Desk y solución de problemas
  - ❏ Gestión de vales de ayuda
  - ❏ Solución de problemas remota
  - ❏ Resolución de problemas remota
  - ❏ Recuperación de desastres en el sistema cliente
- Software y gestión de operaciones
  - ❏ Gestión continuada de equipos de sobremesa
  - ❏ Distribución de software en sistemas HP
  - ❏ Autoreparación de aplicaciones

En determinados modelos de sobremesa y de portátiles, se incluye un agente de gestión Altiris como parte de la imagen cargada en fábrica. Este agente permite la comunicación con la solución de desarrollo de Altiris, la cual se puede utilizar para completar la distribución de hardware nuevo o la migración de personalidad a un sistema operativo nuevo con asistentes fáciles de seguir. Las soluciones Altiris proporcionan capacidades de distribución de software de fácil utilización. Cuando se utiliza junto con System Software Manager, o HP Client Manager, los administradores también pueden actualizar la ROM BIOS y el software de controlador de dispositivo desde una consola central.

Para obtener más información, visite http://www.hp.com/go/easydeploy.

Altiris PC Transplant Pro

Altiris PC Transplant Pro permite efectuar una migración de PC de forma sencilla ya que mantiene los valores, las preferencias y los datos anteriores, y los migra al nuevo entorno rápida y fácilmente. Las actualizaciones tardan solamente minutos en lugar de horas o días, y el funcionamiento y el aspecto del escritorio son los esperados por los usuarios.

Para más información y detalles sobre cómo descargar una versión de evaluación de 30 días con todas las funciones, visite http://h18000.www1.hp.com/im/prodinfo.html#deploy.

System Software Manager

System Software Manager (SSM) es una utilidad que permite actualizar el software del sistema de varios sistemas simultáneamente. Cuando se ejecuta en un sistema de cliente PC, SSM detecta tanto la versión de hardware como la de software y, a continuación, actualiza el software correspondiente desde un repositorio central, también denominado almacén de archivos. Las versiones de controladores que admite SSM se indican mediante un icono especial en la página Web de descarga de controladores y en el CD de software de soporte. Para descargar la utilidad o para obtener más información sobre SSM, visite http://h18000.www1.hp.com/im/ssmwp.html.

Proactive Change Notification

El programa de notificación de cambios proactiva de HP (HP Proactive Change Notification) utiliza la página Web de Subscriber's Choice para, de una forma proactiva y automática, lograr:

- Enviar mensajes de correo electrónico PCN (Proactive Change Notification o Notificación de cambios proactiva) informándole de los cambios en el hardware y el software que tendrán lugar en la mayoría de los ordenadores y servidores del mercado hasta con 60 días de antelación.
- Enviar mensajes de correo electrónico que contienen boletines para el cliente, consejos para el cliente, notas para el cliente, boletines de seguridad y alertas de controladores para la mayoría de los ordenadores y servidores del mercado.

El usuario crea su propio perfil para garantizar que sólo recibe la información relevante para el entorno informático concreto. Para obtener más información sobre el programa Proactive Change Notification y crear un perfil personalizado, visite http://www.hp.com/go/pcn.

ActiveUpdate

ActiveUpdate es una aplicación basada en el cliente de HP. El cliente ActiveUpdate funciona en el sistema local y utiliza el perfil definido por el usuario para descargar de forma proactiva y automática actualizaciones de software para la mayoría de los equipos y servidores de HP en el mercado. Estas actualizaciones de software descargadas se pueden distribuir inteligentemente en las máquinas en las que HP Client Manager Software y System Software Manager tienen previsto instalarlas.

Para obtener más información sobre ActiveUpdate, descargar la aplicación y crear un perfil personalizado, visite: http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html.

Memoria flash de la ROM

El equipo se entrega con una memoria flash de la ROM (memoria de sólo lectura) programable. Es posible establecer una contraseña de configuración en la utilidad Computer Setup (F10) para proteger la ROM ante actualizaciones o sobrescrituras no deseadas. Esto es importante para garantizar la integridad operativa del equipo. Si necesita o desea actualizar la ROM, puede:

- Solicitar un disquete ROMPaq actualizado a HP.
- Descargar las últimas imágenes ROMPaq de http://h18000.www1.hp.com/im/ssmwp.html.

PRECAUCIÓN: para garantizar la máxima protección de la ROM, asegúrese de establecer una contraseña de configuración. La contraseña de configuración impide cualquier actualización de la ROM no autorizada. System Software Manager permite al administrador del sistema establecer una contraseña de configuración en uno o más equipos simultáneamente. Para obtener más información, visite http://h18000.www1.hp.com/im/ssmwp.html.

Memoria flash de la ROM remota

Gracias a la memoria flash de la ROM remota, el administrador del sistema puede actualizar de forma segura la memoria ROM de equipos HP remotos desde la consola de gestión de red centralizada. Al permitir al administrador del sistema realizar esta tarea de forma remota en varios equipos y PC, se consigue una distribución coherente y un mayor control de las imágenes de la memoria ROM de PC de HP en toda la red. También se logra una mayor productividad y un menor coste total de propiedad.

El equipo debe estar encendido, o en estado de activación remota, para poder aprovechar la memoria flash de la ROM remota.

Para obtener más información sobre la memoria flash de la ROM remota, consulte el software HP Client Manager Software o System Software Manager en la página Web http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

La utilidad HPQFlash se utiliza para actualizar o restaurar localmente la ROM del sistema en equipos individuales a través del sistema operativo Windows.

Para obtener más información sobre HPQFlash, visite http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html.

FailSafe Boot Block ROM

La herramienta FailSafe Boot Block ROM permite la recuperación del sistema en el caso poco probable de que se produjera un fallo en la memoria flash de la ROM, como por ejemplo, un corte de alimentación durante la actualización de la ROM. El bloque de arranque es una sección protegida de la memoria flash de la ROM que comprueba si existe una memoria flash válida cuando se enciende el sistema.

- Si la ROM del sistema es válida, el sistema se inicia normalmente.
- Si la ROM del sistema no pasa la comprobación de validación, FailSafe Boot Block ROM proporcionará soporte suficiente para iniciar el sistema desde un disquete ROMPaq, que programará la ROM del sistema con una imagen válida.

Cuando el bloque de arranque detecta que la ROM del sistema no es válida, los indicadores luminosos de alimentación del sistema parpadean en ROJO 8 veces, una por segundo, seguidas de una pausa de 2 segundos. Además, se oirán 8 pitidos al mismo tiempo. Se visualizará un mensaje del modo de recuperación de bloque de arranque en la pantalla (determinados modelos).

Para recuperar el sistema cuando se encuentra en modo de recuperación de bloque de arranque, siga los pasos siguientes:

1. Si hay un disquete en la disquetera, sáquelo y apague el equipo.
2. Inserte un disquete ROMPaq en la unidad correspondiente.
3. Encienda el sistema.
4. Si el sistema no detecta ningún disquete ROMPaq, le solicitará que inserte uno y reinicie el equipo.

5. Si ha establecido una contraseña de configuración, el indicador luminoso Bloq Mayús se encenderá y el sistema solicitará que introduzca la contraseña.
6. Introduzca la contraseña de configuración.
7. Si el sistema se inicia satisfactoriamente desde el disquete y vuelve a programar la ROM, se encenderán los tres indicadores luminosos del teclado. Una serie de tonos ascendentes indican también que el proceso ha finalizado correctamente.
8. Extraiga el disquete y apague el equipo.
9. Vuelva a encenderlo para reiniciar el ordenador.

En la siguiente tabla se indican las diversas combinaciones de los indicadores luminosos del teclado utilizadas por la ROM de bloque de arranque (cuando hay conectado un teclado PS/2 al equipo), y explica el significado y la acción asociada con cada combinación.

Combinaciones de indicadores luminosos del teclado utilizadas por la ROM de bloque de arranque

Modo de bloque de arranque de seguridad	Color del indicador luminoso del teclado	Indicador luminoso de actividad del teclado	Estado/Mensaje
Bloq Num	Verde	Encendido	Disquete ROMPaq no presente, defectuoso o unidad no preparada.
Bloq Mayús	Verde	Encendido	Introduzca la contraseña.
Bloq Num, Bloq Mayús, Bloq Despl	Verde	Secuencia de parpadeo de actividad, uno por uno: Num, Mayús, Despl	Teclado bloqueado en modo de red.
Bloq Num, Bloq Mayús, Bloq Despl	Verde	Encendido	Bloque de arranque de la memoria flash de la ROM satisfactorio. Apague el equipo y, a continuación, enciéndalo para reiniciar.

✎ Los indicadores luminosos de diagnóstico no parpadean en los teclados USB.

Replicación de la configuración

Los procedimientos siguientes permiten al administrador copiar fácilmente una configuración en otros equipos del mismo modelo. Esto hace posible una configuración más rápida y más coherente de varios equipos.

Ambos procedimientos requieren una unidad de disquete o un dispositivo de soporte flash USB compatible, como un módulo de almacenamiento HP Drive Key.

Copiado a un solo equipo

PRECAUCIÓN: cada configuración está diseñada para un modelo específico. Si los equipos de origen y de destino no son del mismo modelo, puede resultar en un sistema de archivos dañado. Por ejemplo, no copie la configuración de un equipo de sobremesa D510 Ultra-slim en un D510 e-pc.

1. Seleccione la configuración que desea copiar. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde. Pulse **Intro** para omitir la pantalla de título, si procede.

Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

3. Inserte un disquete o un dispositivo de soporte flash USB.
4. Haga clic en **File > Save to Diskette** (**Archivo Guardar en disquete**). Siga las instrucciones que aparecen en pantalla para crear el disquete de configuración o el dispositivo de soporte flash USB.
5. Apague el equipo que se va a configurar e inserte el disquete de configuración o el dispositivo de soporte flash USB.
6. Encienda el equipo que se va a configurar. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde. Pulse **Intro** para omitir la pantalla de título, si procede.

7. Haga clic en **File > Restore from Diskette** (**Archivo > Restaurar desde disquete**) y siga las instrucciones de la pantalla.
8. Reinicie el equipo cuando termine la configuración.

Copiado a varios equipos

PRECAUCIÓN: cada configuración está diseñada para un modelo específico. Si los equipos de origen y de destino no son del mismo modelo, puede resultar en un sistema de archivos dañado. Por ejemplo, no copie la configuración de un equipo de sobremesa D510 Ultra-slim en un D510 e-pc.

Con este método se tarda un poco más en preparar el disquete de configuración o el dispositivo de soporte flash USB, pero el proceso de copiar la configuración en los equipos de destino es bastante más rápida.

En Windows 2000 no se puede crear un disco de arranque. Para este procedimiento o para crear un dispositivo de soporte flash USB de arranque se requiere un disquete de arranque. Si no puede utilizar un equipo con Windows 9x ni Windows XP para crear un disquete de arranque, utilice en su lugar el método para copiar a un solo equipo (consulte "Copiado a un solo equipo" en la página 10).

1. Cree un disquete o un dispositivo de soporte flash USB de arranque. Consulte "Disquete de arranque" en la página 12, "Dispositivo de soporte flash USB compatible" en la página 13 o "Dispositivo de soporte flash USB no compatible" en la página 16.

PRECAUCIÓN: no todos los equipos se pueden arrancar desde un dispositivo de soporte flash USB. Si el orden de arranque predeterminado de la utilidad Computer Setup (F10) antepone el dispositivo USB a la unidad de disco duro, el equipo se puede arrancar desde un dispositivo de soporte flash USB. En caso contrario, habrá que utilizar un disquete de arranque.

2. Seleccione la configuración que desea copiar. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.

3. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde. Pulse **Intro** para omitir la pantalla de título, si procede.

Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

4. Inserte el disquete o el dispositivo de soporte flash USB de arranque.
5. Haga clic en **File > Save to Diskette** (**Archivo > Guardar en disquete**). Siga las instrucciones que aparecen en pantalla para crear el disquete o el dispositivo de soporte flash USB de configuración.
6. Descargue una utilidad del BIOS para replicar la configuración (repset.exe) y cópiela en el disquete o dispositivo de soporte flash USB de configuración. Esta utilidad se encuentra en http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html.
7. En el disquete o dispositivo de soporte flash USB de configuración, cree un archivo autoexec.bat que contenga el comando siguiente:

   repset.exe

8. Apague el equipo que se va a configurar. Inserte el disquete o dispositivo de soporte flash USB de configuración y encienda el equipo. La utilidad de configuración se ejecutará automáticamente.
9. Reinicie el equipo cuando termine la configuración.

Creación de un dispositivo de arranque

Disquete de arranque

Estas instrucciones son para Windows XP Professional y Home Edition. Windows 2000 no admite la creación de disquetes de arranque.

1. Inserte un disquete en la unidad de disquete.
2. Haga clic en **Inicio** y, a continuación, haga clic en **Mi PC**.
3. Haga clic con el botón derecho del ratón en la unidad de disquete y luego en **Formatear**.

4. Seleccione la casilla de verificación **Crear un disco de inicio de MS-DOS** y haga clic en **Iniciar**.

Regrese a "Copiado a varios equipos" en la página 11.

Dispositivo de soporte flash USB compatible

Los dispositivos compatibles, como HP Drive Key o DiskOnKey, tienen una imagen preinstalada para simplificar el proceso de convertirlos en dispositivos de arranque. Si el módulo de almacenamiento Drive Key que se está utilizando no tiene esta imagen, utilice el procedimiento que se explica más adelante en esta sección (consulte "Dispositivo de soporte flash USB no compatible" en la página 16).

PRECAUCIÓN: no todos los equipos se pueden arrancar desde un dispositivo de soporte flash USB. Si el orden de arranque predeterminado de la utilidad Computer Setup (F10) antepone el dispositivo USB a la unidad de disco duro, el equipo se puede arrancar desde un dispositivo de soporte flash USB. En caso contrario, habrá que utilizar un disquete de arranque.

Para crear un dispositivo de soporte flash USB, debe tener:

- Uno de los siguientes sistemas:
  - Equipo de sobremesa Compaq Evo D510 Ultra-slim
  - Equipos de formato reducido/minitorre convertible Compaq Evo D510
  - Equipo de sobremesa para empresas serie d530 de HP Compaq – equipo de sobremesa Ultra-slim, equipo de formato reducido o minitorre convertible
  - Equipos portátiles Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c o N1000c
  - Equipos portátiles Compaq Presario 1500 o 2800

  Dependiendo del BIOS individual, los sistemas del futuro también podrán admitir el arranque desde el módulo de almacenamiento HP Drive Key.

PRECAUCIÓN: si está utilizando un equipo distinto a los mencionados anteriormente, asegúrese de que el orden de arranque predeterminado en la utilidad Computer Setup (F10) antepone el dispositivo USB a la unidad de disco.

- Uno de los siguientes módulos de almacenamiento:
  - HP Drive Key de 16 MB
  - HP Drive Key de 32 MB
  - DiskOnKey de 32 MB
  - HP Drive Key de 64 MB
  - DiskOnKey de 64 MB
  - HP Drive Key de 128 MB
  - DiskOnKey de 128 MB
- Un disquete DOS de arranque con los programas FDISK y SYS. Si el programa SYS no está disponible, puede utilizar FORMAT pero todos los archivos existentes en el módulo de almacenamiento Drive Key se perderán.

1. Apague el ordenador.
2. Conecte el módulo de almacenamiento Drive Key en uno de los puertos USB del equipo y desconecte el resto de los dispositivos de almacenamiento USB a excepción de las unidades de disquete USB.
3. Inserte un disquete DOS de arranque con FDISK.COM y con SYS.COM o FORMAT.COM en una unidad de disquete y encienda el equipo para arrancar desde el disquete DOS.
4. Ejecute FDISK desde el comando A:\ escribiendo **FDISK** y pulsando Intro. Si se le indica, haga clic en la opción afirmativa **Yes** (**Y**) para activar la compatibilidad con discos de gran tamaño.
5. Introduzca la opción [**5**] para que aparezcan las unidades del sistema. Drive Key será el módulo que mejor coincida con el tamaño de una de las unidades que se indican en la lista. Normalmente, es la última unidad de la lista. Tome nota de la letra de la unidad.

   Módulo de almacenamiento Drive Key: _____

PRECAUCIÓN: si no hay una unidad que coincida con el módulo Drive Key, no siga adelante. Se podrían perder los datos. Compruebe todos los puertos USB para ver los dispositivos de almacenamiento adicionales. Si encuentra alguno, extráigalo, reinicie el equipo y siga en el paso 4. Si no se encuentra niguno, el sistema no es compatible con el módulo de almacenamiento Drive Key o el que está instalado está dañado. NO siga intentando hacer que el sistema arranque desde el módulo Drive Key.

6. Salga de FDISK pulsando la tecla **Esc** para regresar al comando A:\.
7. Si el disquete DOS de arranque contiene SYS.COM, continúe en el paso 8. En caso contrario, siga en el paso 9.
8. En el comando A:\ introduzca **SYS x:** donde x representa la letra de la unidad que anotó anteriormente. Continúe en el paso 13.

PRECAUCIÓN: asegúrese de que ha introducido la letra de unidad correcta para el módulo de almacenamiento Drive Key.

Después de transferir los archivos de sistema, SYS regresará al comando A:\.

9. Copie los archivos que desee guardar del módulo de almacenamiento Drive Key en un directorio temporal de otra unidad (por ejemplo, la unidad de disco duro interno del sistema).
10. En el comando A:\ introduzca **FORMAT /S X:** donde X representa la letra de la unidad que anotó anteriormente.

PRECAUCIÓN: asegúrese de que ha introducido la letra de unidad correcta para el módulo de almacenamiento Drive Key.

El comando FORMAT le mostrará uno o varios mensajes de advertencia y le preguntará cada vez si desea continuar. Introduzca **y** cada vez. FORMAT formateará el módulo de almacenamiento Drive Key, agregará los archivos de sistema y le pedirá una Etiqueta de volumen.

11. Pulse **Intro** si no desea asignar ninguna etiqueta o introduzca una si así lo desea.
12. Vuelva a copiar los archivos que guardó en el paso 9 en el módulo de almacenamiento Drive Key.

13. Extraiga el disquete y reinicie el equipo. El equipo arrancará el módulo de almacenamiento Drive Key como unidad principal C.

El orden de arranque predeterminado varía de un equipo a otro, y se puede cambiar mediante la utilidad Computer Setup (F10).

Si ha utilizado una versión DOS de Windows 9x, es posible que aparezca brevemente una pantalla con el logotipo Windows. Si no desea que aparezca esta pantalla, agregue un archivo de longitud cero llamado LOGO.SYS al directorio raíz del módulo de almacenamiento Drive Key.

Regrese a "Copiado a varios equipos" en la página 11.

Dispositivo de soporte flash USB no compatible

PRECAUCIÓN: no todos los equipos se pueden arrancar desde un dispositivo de soporte flash USB. Si el orden de arranque predeterminado de la utilidad Computer Setup (F10) antepone el dispositivo USB a la unidad de disco duro, el equipo se puede arrancar desde un dispositivo de soporte flash USB. En caso contrario, habrá que utilizar un disquete de arranque.

Para crear un dispositivo de soporte flash USB, debe tener:

- Uno de los siguientes sistemas:
  - Equipo de sobremesa Compaq Evo D510 Ultra-slim
  - Equipos de formato reducido/minitorre convertible Compaq Evo D510
  - Equipo de sobremesa para empresas serie d530 de HP Compaq – equipo de sobremesa Ultra-slim, equipo de formato reducido o minitorre convertible
  - Equipos portátiles Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c o N1000c
  - Equipos portátiles Compaq Presario 1500 o 2800

  Dependiendo del BIOS individual, los sistemas del futuro también podrán admitir el arranque desde el dispositivo de soporte flash USB.

PRECAUCIÓN: si está utilizando un equipo distinto a los mencionados anteriormente, asegúrese de que el orden de arranque predeterminado en la utilidad Computer Setup (F10) antepone el dispositivo USB a la unidad de disco.

- Un disquete DOS de arranque con los programas FDISK y SYS. Si el programa SYS no está disponible, puede utilizar FORMAT pero todos los archivos existentes en el módulo de almacenamiento Drive Key se perderán.

1. Si hay alguna tarjeta PCI en el sistema que tenga conectadas unidades SCSI, ATA RAID o SATA, apague el equipo y desenchufe el cable de alimentación.

PRECAUCIÓN: el cable de alimentación DEBE estar desenchufado.

2. Abra el equipo y extraiga las tarjetas PCI.
3. Conecte el dispositivo de soporte flash USB en uno de los puertos USB del equipo y desconecte el resto de los dispositivos de almacenamiento USB a excepción de las unidades de disquete USB. Ponga la cubierta del equipo.
4. Enchufe el cable de alimentación y encienda el equipo. Tan pronto como la luz del monitor se ponga en verde, pulse la tecla **F10** para entrar en la utilidad Computer Setup.
5. Acceda a Advanced/PCI devices (Avanzado/Dispositivos PCI) para desactivar los controladores IDE y SATA. Cuando desactive el controlador SATA, tome nota del IRQ al que está asignado el controlador. Tendrá que volver a asignar el IRQ más tarde. Salga de la configuración, confirmando los cambios realizados.

   SATA IRQ: _____
6. Inserte un disquete DOS de arranque con FDISK.COM y con SYS.COM o FORMAT.COM en una unidad de disquete y encienda el equipo para arrancar desde el disquete DOS.
7. Ejecute FDISK y elimine cualquier partición existente en el dispositivo de soporte flash USB. Cree una partición nueva y márquela como activa. Salga de FDISK pulsando la tecla **Esc**.
8. Si al salir de FDISK el sistema no se reinicia automáticamente, pulse **Ctrl+Alt+Del** para reiniciar desde el disquete DOS.

9. En el comando A:\ escriba **FORMAT C: /S** y pulse **Intro**. FORMAT formateará el dispositivo de soporte flash USB, agregará los archivos de sistema y le pedirá una Etiqueta de volumen.
10. Pulse **Intro** si no desea asignar ninguna etiqueta o introduzca una si así lo desea.
11. Apague el equipo y desenchufe el cable de alimentación. Abra el equipo y vuelva a instalar las tarjetas PCI que extrajo anteriormente. Ponga la cubierta del equipo.
12. Enchufe el cable de alimentación, saque el disquete y encienda el equipo.
13. Tan pronto como la luz del monitor se ponga en verde, pulse la tecla **F10** para entrar en la utilidad Computer Setup.
14. Acceda a Advanced/PCI devices (Avanzado/Dispositivos PCI) y vuelva a activar los controladores IDE y SATA que desactivó en el paso 5. Ponga el controlador SATA en su IRQ original.
15. Guarde los cambios y salga. El equipo arrancará desde el dispositivo de soporte flash USB como unidad principal C.

El orden de arranque predeterminado varía de un equipo a otro, y se puede cambiar mediante la utilidad Computer Setup (F10).

Si ha utilizado una versión DOS de Windows 9x, es posible que aparezca brevemente una pantalla con el logotipo Windows. Si no desea que aparezca esta pantalla, agregue un archivo de longitud cero llamado LOGO.SYS al directorio raíz del módulo de almacenamiento Drive Key.

Regrese a "Copiado a varios equipos" en la página 11.

Botón de encendido de modo dual

Si la interfaz ACPI (interfaz de alimentación y configuración avanzada) está activada para Windows 2000, Windows XP Professional y Home Edition, el botón de encendido puede funcionar como botón de encendido o de apagado, o como botón de suspensión. La función de suspensión no apaga completamente el equipo, sino que hace que entre en modo de estado de espera de bajo consumo. Esto permite apagar rápidamente el sistema sin tener que cerrar las aplicaciones y volver rápidamente al mismo estado operativo en que se encontraba sin que se produzcan pérdidas de datos.

Para cambiar la configuración del botón de encendido, siga estos pasos:

1. En Windows 2000, haga clic con el botón izquierdo del ratón en el botón **Inicio**, seleccione **Configuración > Panel de control > Opciones de energía**.

   En Windows XP Professional y Home Edition, haga clic con el botón izquierdo del ratón en el botón **Inicio,** seleccione **Panel de control > Rendimiento y mantenimiento > Opciones de energía**.

2. En las **Propiedades de las Opciones de energía** seleccione la pestaña **Avanzado**.

3. En la sección **Botones de encendido**, seleccione la configuración deseada para el botón de encendido.

Tras configurar el botón de encendido para que funcione como un botón de suspensión, pulse el botón de encendido para que el sistema pase al estado de ahorro de energía (suspendido). Pulse el botón de nuevo para que el sistema pase rápidamente al estado normal de funcionamiento. Para apagar completamente el sistema, mantenga pulsado el botón de encendido durante cuatro segundos.

PRECAUCIÓN: no utilice el botón de encendido para apagar el ordenador a menos que el sistema no responda; si apaga el equipo sin la interacción del sistema operativo, podría dañar el disco duro o perder datos.

Página Web

Los ingenieros de HP prueban de forma rigurosa y depuran el software desarrollado por HP y otros fabricantes, y desarrollan software de soporte específico para el sistema operativo a fin de garantizar el nivel de rendimiento, compatibilidad y fiabilidad de los equipos de HP.

Cuando se realiza la transición a sistemas operativos nuevos o revisados, es importante implementar el software de soporte diseñado para el sistema operativo en cuestión. Si pretende ejecutar una versión de Microsoft Windows que no sea la versión incluida con el equipo, deberá instalar los controladores de dispositivo y las utilidades correspondientes para garantizar la compatibilidad y el funcionamiento adecuado de todas las funciones.

HP ha facilitado la tarea de localizar, acceder, evaluar e instalar el software de soporte más reciente. Puede decargar el software de http://www.hp.com/support.

La página Web contiene los controladores de dispositivo, las utilidades y las imágenes de la memoria flash de la ROM más actuales necesarios para ejecutar el sistema operativo Microsoft Windows más reciente en el equipo de HP.

Productos base y empresas colaboradoras

Las soluciones de gestión de HP se integran con otras aplicaciones de gestión de sistemas y se basan en estándares de la industria como:

- Desktop Management Interface (DMI) 2.0
- Tecnología WOL (Wake on LAN)
- ACPI
- SMBIOS
- Soporte de ejecución previa al arranque (PXE)

Seguridad y seguimiento de activos

Las funciones de seguimiento de activos incorporadas en el equipo proporcionan datos de seguimiento de activos clave que se pueden gestionar con HP Insight Manager, HP Client Manager u otras aplicaciones de administración de sistemas. Del mismo modo, la integración automática entre las funciones de seguimiento de activos y dichos productos permite seleccionar la herramienta de gestión que mejor se adapta al entorno y equilibrar la inversión en herramientas existentes.

HP también ofrece varias soluciones para controlar el acceso a componentes e información valiosos. La función de seguridad integrada ProtectTools, si está instalada, impide el acceso no autorizado a los datos y comprueba la integridad del sistema, y autentifica los usuarios externos que intentan acceder al sistema. Las características de seguridad (como ProtectTools, el sensor de Smart Cover y el bloqueo de Smart Cover) disponibles en determinados modelos, ayudan a impedir el acceso no autorizado a los componentes internos del equipo. Para proteger los activos de datos valiosos, desactive los puertos paralelo, serie o USB, o bien las capacidades de arranque de soporte extraíble. Las alertas de cambio de memoria y del sensor de Smart Cover pueden enviarse automáticamente a aplicaciones de gestión de sistemas para enviar una notificación proactiva de seguridad con un componente interno del equipo.

ProtectTools, el sensor y el bloqueo de Smart Cover están disponibles como opciones en determinados sistemas.

Use las utilidades siguientes para gestionar valores de seguridad en el equipo de HP:

- De forma local, mediante las utilidades de Computer Setup. Para obtener información adicional e instrucciones sobre cómo utilizar las utilidades de Computer Setup, consulte la publicación *Guía sobre la utilidad Computer Setup (F10)* que se entrega con el equipo.
- De forma remota, con HP Client Manager o System Software Manager. Este software permite distribuir, de forma segura y coherente, y controlar los valores de seguridad de una sencilla utilidad de línea de comandos.

La tabla y las secciones siguientes hacen referencia a la gestión de características de seguridad del equipo, de forma local, mediante las utilidades de Computer Setup (F10).

Descripción general de las características de seguridad

Elemento	Objetivo	Cómo se establece
Removable Media Boot Control (Control de arranque desde soporte extraíble)	Impedir el arranque desde unidades de soporte extraíbles (disponible en determinadas unidades)	Desde el menú de utilidades de Computer Setup (F10).
Serial, Parallel, USB or Infrared Interface Control (Control de las interfaces serie, paralela, USB o de infrarrojos)	Impedir la transferencia de datos a través de las interfaces integradas serie, paralela, USB o de infrarrojos.	Desde el menú de utilidades de Computer Setup (F10).
Power-On Password (Contraseña de arranque)	Impedir que se utilice el equipo si no se ha introducido la contraseña. Esto es válido tanto para el arranque inicial del sistema como para cualquier reinicio.	Desde el menú de utilidades de Computer Setup (F10).
Setup Password (Contraseña de configuración)	Impedir que se modifique la configuración del equipo (uso de las utilidades de Computer Setup) si no se ha introducido la contraseña.	Desde el menú de utilidades de Computer Setup (F10).
Embedded Security Device (Dispositivo de seguridad integrada)	Evitar el acceso no autorizado a los datos mediante el uso de codificación y protección con contraseña. Comprobar la integridad del sistema y autentificar los usuarios externos que intentan acceder al sistema.	Desde el menú de utilidades de Computer Setup (F10).

✎ Para obtener más información sobre Computer Setup, consulte la publicación *Guía sobre la utilidad Computer Setup (F10)*.

Las funciones de seguridad admitidas pueden variar según la configuración específica del equipo.

Descripción general de las características de seguridad *(Continuación)*

Elemento	Objetivo	Cómo se establece
DriveLock (Bloqueo de la unidad)	Impedir el acceso no autorizado a los datos de unidades de disco duro de compartimiento multiuso. Esta función sólo está disponible en determinados modelos.	Desde el menú de utilidades de Computer Setup (F10).
Smart Cover Sensor (Sensor de Smart Cover)	Indicar que se ha extraído la cubierta o el panel lateral del equipo. Se puede configurar para que solicite la contraseña de configuración para reiniciar el equipo, una vez extraída la cubierta o el panel lateral. Para obtener más información sobre esta función, consulte la publicación *Guía de referencia del hardware* en el CD *Biblioteca de documentación*. Esta función sólo está disponible en determinados modelos.	Desde el menú de utilidades de Computer Setup (F10).
Master Boot Record Security (Seguridad del registro de arranque maestro)	Impedir que se efectúen cambios no intencionados o maliciosos en el registro de arranque maestro del disco de arranque actual, y proporcionar un medio para recuperar el último registro maestro de arranque correcto.	Desde el menú de utilidades de Computer Setup (F10).

✎ Para obtener más información sobre Computer Setup, consulte la publicación *Guía sobre la utilidad Computer Setup (F10)*.

Las funciones de seguridad admitidas pueden variar según la configuración específica del equipo.

Descripción general de las características de seguridad *(Continuación)*

Elemento	Objetivo	Cómo se establece
Memory Change Alerts (Alertas de cambio de memoria)	Detectar si se han añadido, movido o extraído módulos de memoria, y notificar estos cambios al usuario y al administrador del sistema.	Para obtener más información sobre cómo activar las alertas de cambio de memoria, consulte la publicación en línea *Intelligent Manageability Guide* (Guía de Intelligent Manageability).
Ownership Tag (Identificador de propiedad)	Mostrar la información de propiedad, según la definición del administrador del sistema, al arrancar el sistema (protegido por la contraseña de configuración).	Desde el menú de utilidades de Computer Setup (F10).
Cable Lock Provision (Candado con cadena)	Inhibir el acceso al interior del equipo para impedir cambios de configuración no deseados o la extracción de componentes. También se puede utilizar para fijar el equipo a un elemento fijo a fin de impedir un posible robo.	Instalando una cadena para fijar el equipo a un elemento fijo.
Security Loop Provision (Bucle de seguridad)	Inhibir el acceso al interior del equipo para impedir cambios de configuración no deseados o la extracción de componentes.	Instalando un candado en el bucle de seguridad para impedir cambios de configuración no deseados o la extracción de componentes.

✎ Para obtener más información sobre Computer Setup, consulte la publicación *Guía sobre la utilidad Computer Setup (F10)*.

Las funciones de seguridad admitidas pueden variar según la configuración específica del equipo.

Seguridad mediante contraseña

La contraseña de arranque impide la utilización no autorizada del equipo ya que se solicita la introducción de una contraseña para acceder a aplicaciones o a datos cada vez que se enciende o reinicia el equipo. La contraseña de configuración impide específicamente el acceso no autorizado a Computer Setup, y también se puede utilizar en sustitución de la contraseña de arranque. Es decir, si cuando se solicita la contraseña de arranque se introduce en su lugar la contraseña de configuración, se podrá acceder igualmente al equipo.

Se puede establecer una contraseña de configuración para toda la red para que el administrador del sistema pueda conectarse a todos los sistemas de red y realizar tareas de mantenimiento sin necesidad de conocer la contraseña de arranque, aunque se haya definido una.

Definición de una contraseña de configuración mediante Computer Setup

Si el sistema está equipado con un dispositivo de seguridad integrada, consulte "Seguridad integrada" en la página 30.

La definición de una contraseña de configuración mediante Computer Setup evita tener que configurar de nuevo el equipo (uso de la utilidad Computer Setup (F10)) hasta que se haya introducido la contraseña.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde. Pulse **Intro** para omitir la pantalla de título, si procede.

Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

3. Seleccione **Security** (**Seguridad**) y, a continuación, **Setup Password** (**Contraseña de configuración**), y siga las instrucciones que aparecen en la pantalla.
4. Antes de salir, haga clic en **File > Save Changes** and **Exit** (**Archivo > Guardar cambios** y **Salir**).

Definición de una contraseña de arranque mediante Computer Setup

La definición de una contraseña de arranque mediante Computer Setup impide el acceso al equipo cuando está encendido si no se introduce la contraseña. Si se ha establecido una contraseña de arranque, podrá seleccionar Password Options (Opciones de contraseña) en el menú Security (Seguridad) de Computer Setup. Las opciones de contraseña incluyen la Solicitud de contraseña durante un arranque en caliente. Si se ha activado la solicitud de contraseña durante un arranque en caliente, la contraseña también debe introducirse cada vez que se reinicia el equipo.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde. Pulse **Intro** para omitir la pantalla de título, si procede.

Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

3. Seleccione **Security** (**Seguridad**) y, a continuación, **Power-On Password** (**Contraseña de arranque**), y siga las instrucciones que aparecen en la pantalla.
4. Antes de salir, haga clic en **File > Save Changes** and **Exit** (**Archivo > Guardar cambios** y **Salir**).

Introducción de una contraseña de arranque

Para introducir una contraseña de arranque, siga estos pasos:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Cuando aparezca el icono de llave en la pantalla, escriba la contraseña actual y, a continuación, pulse **Intro**.

Preste atención al escribir la contraseña puesto que, por motivos de seguridad, los caracteres que se escriben no aparecen en la pantalla.

Si la contraseña introducida no es correcta, aparecerá un icono de llave rota. Inténtelo de nuevo. Al cabo de tres intentos sin éxito, deberá apagar el equipo y volver a encenderlo para poder continuar.

Introducción de una contraseña de configuración

Si el sistema está equipado con un dispositivo de seguridad integrada, consulte "Seguridad integrada" en la página 30.

Si se ha establecido una contraseña de configuración en el equipo, dicha contraseña se solicitará cada vez que se ejecute Computer Setup.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde.

Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

3. Cuando aparezca el icono de llave en la pantalla, escriba la contraseña de configuración y, a continuación, pulse la tecla **Intro**.

Preste atención al escribir la contraseña puesto que, por motivos de seguridad, los caracteres que se escriben no aparecen en la pantalla.

Si la contraseña introducida no es correcta, aparecerá un icono de llave rota. Inténtelo de nuevo. Al cabo de tres intentos sin éxito, deberá apagar el equipo y volver a encenderlo para poder continuar.

Modificación de una contraseña de arranque o de configuración

Si el sistema está equipado con un dispositivo de seguridad integrada, consulte "Seguridad integrada" en la página 30.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**. Para modificar la contraseña de configuración, ejecute **Computer Setup**.
2. Cuando aparezca el icono de llave, escriba la contraseña actual, una barra inclinada (/) o un carácter delimitador alternativo, la nueva contraseña, otra barra inclinada (/) o un carácter delimitador alternativo, y otra vez la nueva contraseña, tal como se indica a continuación:
   contraseña actual/nueva contraseña/nueva contraseña

Preste atención al escribir la contraseña puesto que, por motivos de seguridad, los caracteres que se escriben no aparecen en la pantalla.

3. Pulse la tecla **Intro**.

La nueva contraseña se aplicará la próxima vez que encienda el equipo.

Consulte "Caracteres delimitadores de un teclado nacional" en la página 29 para obtener más información sobre los caracteres delimitadores alternativos. La contraseña de arranque y la contraseña de configuración también pueden modificarse mediante las opciones de seguridad de Computer Setup.

Eliminación de una contraseña de arranque o de configuración

Si el sistema está equipado con un dispositivo de seguridad integrada, consulte "Seguridad integrada" en la página 30.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**. Para eliminar la contraseña de configuración, ejecute **Computer Setup**.

2. Cuando aparezca el icono de llave, escriba la contraseña actual seguida de una barra inclinada (/) o un carácter delimitador alternativo, tal como se muestra a continuación:
   contraseña actual/
3. Pulse la tecla **Intro**.

Consulte "Caracteres delimitadores de un teclado nacional" para obtener más información sobre los caracteres delimitadores alternativos. La contraseña de arranque y la contraseña de configuración también pueden modificarse mediante las opciones de seguridad de Computer Setup.

Caracteres delimitadores de un teclado nacional

Los distintos teclados se diseñan conforme a los requisitos específicos de cada país. La sintaxis y las teclas que cada usuario utiliza para modificar o eliminar la contraseña dependen del teclado que se entregó con el equipo.

Caracteres delimitadores de un teclado nacional

Árabe	/	Griego	-	Ruso	/
Belga	=	Hebreo	.	Eslovaco	-
BHCSY*	-	Húngaro	-	Español	-
Brasileño	/	Italiano	-	Sueco/Finlandés	/
Chino	/	Japonés	/	Suizo	-
Checo	-	Coreano	/	Taiwanés	/
Danés	-	Latinoamericano	-	Tailandés	/
Francés	!	Noruego	-	Turco	.
Francés canadiense	é	Polaco	-	Inglés británico	/
Alemán	-	Portugués	-	Inglés americano	/

* Bosnia-Hercegovina, Croacia, Eslovenia y Yugoslavia

Cómo borrar contraseñas

Si olvida la contraseña, no podrá acceder al equipo. Para obtener instrucciones acerca de cómo borrar contraseñas, consulte la *Guía de solución de problemas*.

Si el sistema está equipado con un dispositivo de seguridad integrada, consulte "Seguridad integrada."

Seguridad integrada

La función de seguridad integrada ProtectTools combina la codificación y la protección con contraseña para proporcionar una seguridad mejorada para la codificación de carpetas o archivos en el sistema de archivos integrado (EFS, Embedded File System) y el correo electrónico seguro con Microsoft Outlook y Outlook Express. ProtectTools está disponible para determinados equipos de sobremesa como opción que se puede solicitar a la hora de hacer el pedido (CTO, Configured to Order). Está destinado a los clientes de HP cuya preocupación principal son los datos confidenciales. El acceso no autorizado a los datos presenta un peligro mucho mayor que la propia pérdida de los datos. ProtectTools utiliza cuatro contraseñas:

- (F10) Setup: para entrar en la utilidad Computer Setup (F10) y activar/desactivar ProtectTools
- Take Ownership (asignación de propiedad): para que la configure y utilice el administrador del sistema, que autorizará a los usuarios y establecerá los parámetros de seguridad
- Emergency Recovery Token (token de recuperación de emergencia): para que la establezca el administrador del sistema; permitirá la recuperación en caso de que se produzca un fallo del chip ProtectTools o del equipo
- Basic User (usuario básico): para que la establezca y utilice el usuario final

Si se pierde la contraseña de usuario final, los datos codificados no se podrán recuperar. Por lo tanto, la función ProtectTools es especialmente más segura de utilizar cuando los datos contenidos en la unidad del usuario se replican en un sistema de información o se les hace una copia de seguridad periódicamente.

El sistema de seguridad integrada ProtectTools es un chip de seguridad compatible con TCPA 1.1 que se instala de forma opcional en la placa del sistema de determinados equipos de escritorio para empresas. Cada chip ProtectTools es único y está vinculado a un equipo específico. Cada chip realiza procesos de seguridad principales independientes de los componentes de otros equipos (como el procesador, la memoria o el sistema operativo).

Un equipo con la función de seguridad integrada ProtectTools activada complementa y mejora las funciones de seguridad incluidas en Microsoft Windows 2000, Windows XP Professional o Home Edition. Por ejemplo, mientras el sistema operativo puede codificar los archivos y carpetas locales basados en un EFS, la seguridad integrada ProtectTools ofrece una capa adicional de seguridad al crear claves de codificación desde la clave raíz de la plataforma (que se almacena en silicona). Este proceso se conoce como "envolver" las claves de codificación. ProtectTools no impide el acceso de la red a los equipos que no tengan ProtectTools.

Las funciones principales de la seguridad integrada ProtectTools incluyen:

- Autenticación de plataforma
- Almacenamiento protegido
- Integridad de los datos

PRECAUCIÓN: proteja las contraseñas. **No se puede acceder ni recuperar los datos codificados sin las contraseñas**.

Configuración de contraseñas

Configuración

La utilidad de configuración F10 permite crear una contraseña de configuración y activar el dispositivo de seguridad integrada.

1. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde.

Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

2. Utilice la tecla de flecha arriba o abajo para seleccionar un idioma y, a continuación, pulse **Intro**.
3. Utilice la tecla de flecha izquierda o derecha para acceder a la pestaña **Security** (**Seguridad**) y, a continuación, use la tecla de flecha arriba o abajo para acceder a **Setup Password** (**Contraseña de configuración**). Pulse **Intro**.
4. Escriba y confirme una contraseña. Pulse **F10** para aceptar la contraseña.

Preste atención al escribir la contraseña puesto que, por motivos de seguridad, los caracteres que se escriben no aparecen en la pantalla.

5. Utilice la tecla de flecha arriba o abajo para acceder a **Embedded Security Device** (**Dispositivo de seguridad integrada**). Pulse **Intro**.
6. Si en el cuadro de diálogo está seleccionada la opción **Embedded Security Device – Disable** (**Dispositivo de seguridad integrada, desactivado**), utilice la tecla de flecha izquierda o derecha para cambiarlo a **Embedded Security Device – Enable** (**Dispositivo de seguridad integrada, activado**). Pulse **F10** para aceptar el cambio.

PRECAUCIÓN: si selecciona **Reset to Factory Settings – Reset (Restablecer los valores de fábrica, restablecer)**, se eliminarán todas las claves y los datos codificados no se podrán recuperar *a menos que* se haya hecho una copia de seguridad de las claves (consulte "Asignación de propiedad y Token de recuperación de emergencia"). Sólo debe seleccionar **Reset (Restablecer)** cuando se le indique en el procedimiento de recuperación de datos codificados (consulte "Recuperación de datos codificados" en la página 35).

7. Utilice la tecla de flecha izquierda o derecha para acceder a **File** (**Archivo**). Utilice la tecla de flecha arriba o abajo para acceder a **Save Changes and Exit** (**Guardar cambios y Salir**). Pulse **Intro** y, a continuación, pulse **F10** para confirmar.

Asignación de propiedad y Token de recuperación de emergencia

La contraseña de Asignación de propiedad es necesaria para activar o desactivar la plataforma de seguridad y autorizar a los usuarios. Si el dispositivo de seguridad integrada falla, el mecanismo de recuperación de emergencia permite que los usuarios sean autorizados y puedan acceder a los datos.

1. Si utiliza Windows XP Professional o Home Edition, haga clic en **Inicio > Todos los programas > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard** (**Herramientas de seguridad integrada ProtectTools de HP > Asistente para la inicialización de seguridad integrada**).

   Si utiliza Windows 2000, haga clic en **Inicio > Programas > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard** (**Herramientas de seguridad integrada ProtectTools de HP > Asistente para la inicialización de seguridad integrada**).

2. Haga clic en **Siguiente**.
3. Escriba y confirme la contraseña de Asignación de propiedad y, a continuación, haga clic en **Siguiente**.

Preste atención al escribir la contraseña puesto que, por motivos de seguridad, los caracteres que se escriben no aparecen en la pantalla.

4. Haga clic en **Siguiente** para aceptar la ubicación del archivo de recuperación predeterminada.
5. Escriba y confirme la contraseña de Token de recuperación de emergencia y, a continuación, haga clic en **Siguiente**.
6. Inserte un disquete para guardar la clave de Token de recuperación de emergencia. Haga clic en **Examinar** y seleccione el disquete.

PRECAUCIÓN: la clave de Token de recuperación de emergencia se utiliza para recuperar los datos codificados en el caso de que se produzca un fallo en el chip de seguridad integrada o en el equipo. **Los datos no se pueden recuperar sin esta clave**. (No se puede acceder a los datos sin la contraseña de usuario básico.) Guarde este disquete en un lugar seguro.

7. Haga clic en **Guardar** para aceptar la ubicación y el nombre de archivo predeterminado, a continuación, haga clic en **Siguiente**.
8. Haga clic en **Siguiente** para confirmar los valores antes de iniciar la plataforma de seguridad.

Aparecerá un mensaje indicando que las funciones de seguridad integrada no se han iniciado. No haga clic en el mensaje. Esto se tratará más adelante en el procedimiento y el mensaje se cerrará al cabo de unos segundos.

9. Haga clic en **Siguiente** para omitir la configuración de políticas locales.
10. Asegúrese de que la casilla de verificación Start Embedded Security User Initialization Wizard (Abrir el Asistente para la inicialización del usuario de seguridad integrada), a continuación haga clic en **Finish** (**Terminar**).

El asistente para la inicialización de usuario se abre automáticamente.

Usuario básico

Durante la inicialización de usuario se crea la contraseña de usuario básico. Esta contraseña es necesaria para entrar y acceder a los datos codificados.

PRECAUCIÓN: proteja la contraseña de usuario básico. **No se puede acceder ni recuperar los datos codificados sin esta contraseña**.

1. Si el Asistente para la inicialización de usuario no se abre:

   Si utiliza Windows XP Professional o Home Edition, haga clic en **Inicio > Todos los programas > HP ProtectTools Embedded Security Tools > User Initialization Wizard** (**Herramientas de seguridad integrada ProtectTools de HP > Asistente para la inicialización de usuario**).

Si utiliza Windows 2000, haga clic en **Inicio > Programas > HP ProtectTools Embedded Security Tools > User Initialization Wizard** (**Herramientas de seguridad integrada ProtectTools de HP > Asistente para la inicialización de usuario**).

2. Haga clic en **Siguiente**.
3. Escriba y confirme la contraseña de Clave de usuario básico y, a continuación, haga clic en **Siguiente**.

Preste atención al escribir la contraseña puesto que, por motivos de seguridad, los caracteres que se escriben no aparecen en la pantalla.

4. Haga clic en **Siguiente** para confirmar los valores.
5. Seleccione las funciones de seguridad apropiadas y haga clic en **Siguiente**.
6. Haga clic en el cliente de correo electrónico correspondiente para seleccionarlo y, a continuación, haga clic en **Siguiente**.
7. Haga clic en **Siguiente** para aplicar el Certificado de codificación.
8. Haga clic en **Siguiente** para confirmar los valores.
9. Haga clic en **Terminar**.
10. Reinicie el equipo.

Recuperación de datos codificados

Para recuperar los datos después de sustituir el chip de ProtectTools, debe contar con lo siguiente:

- SPEmRecToken.xml: la clave de Token de recuperación de emergencia
- SPEmRecArchive.xml: carpeta oculta, ubicación predeterminada: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- Contraseñas de ProtectTools
  - Configuración
  - Asignación de propiedad
  - Token de recuperación de emergencia
  - Usuario básico

1. Reinicie el equipo.
2. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde.

Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

3. Escriba la contraseña de configuración y, a continuación, pulse **Intro**.
4. Utilice la tecla de flecha arriba o abajo para seleccionar un idioma y, a continuación, pulse **Intro**.
5. Utilice la tecla de flecha izquierda o derecha para acceder a la pestaña **Security** (**Seguridad**) y, a continuación, use la tecla de flecha arriba o abajo para acceder a **Embedded Security Device** (**Dispositivo de seguridad integrada**). Pulse **Intro**.
6. Si sólo hay disponible una opción, **Embedded Security Device – Disable** (**Dispositivo de seguridad integrada, desactivado**):
   a. Utilice la tecla de flecha izquierda o derecha para cambiarla a **Embedded Security Device – Enable** (**Dispositivo de seguridad integrada, activado**). Pulse **F10** para aceptar el cambio.
   b. Utilice la tecla de flecha izquierda o derecha para acceder a **File** (**Archivo**). Utilice la tecla de flecha arriba o abajo para acceder a **Save Changes and Exit** (**Guardar cambios y Salir**). Pulse **Intro** y, a continuación, pulse **F10** para confirmar.
   c. Continúe en el paso 1.

   Si están disponibles las dos opciones, continúe en el paso 7.
7. Utilice la tecla de flecha arriba o abajo para acceder a **Reset to Factory Settings – Do Not Reset** (**Restablecer los valores de fábrica, no restablecer**). Pulse una vez la tecla de flecha izquierda o derecha.

   Aparecerá un mensaje indicando: Si realiza esta acción se restablecerán los valores de fábrica del dispositivo de seguridad integrada si guarda dichos valores al salir. Pulse cualquier tecla para continuar.

   Pulse **Intro**.

8. Ahora la selección aparecerá como **Reset to Factory Settings – Reset** (**Restablecer los valores de fábrica, restablecer**). Pulse **F10** para aceptar el cambio.
9. Utilice la tecla de flecha izquierda o derecha para acceder a **File** (**Archivo**). Utilice la tecla de flecha arriba o abajo para acceder a **Save Changes and Exit** (**Guardar cambios y Salir**). Pulse **Intro** y, a continuación, pulse **F10** para confirmar.
10. Reinicie el equipo.
11. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde.

✎ Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

---

12. Escriba la contraseña de configuración y, a continuación, pulse **Intro**.
13. Utilice la tecla de flecha arriba o abajo para seleccionar un idioma y, a continuación, pulse **Intro**.
14. Utilice la tecla de flecha izquierda o derecha para acceder a la pestaña **Security** (**Seguridad**) y, a continuación, use la tecla de flecha arriba o abajo para acceder a **Embedded Security Device** (**Dispositivo de seguridad integrada**). Pulse **Intro**.
15. Si en el cuadro de diálogo está seleccionada la opción **Embedded Security Device – Disable** (**Dispositivo de seguridad integrada, desactivado**), utilice la tecla de flecha izquierda o derecha para cambiarlo a **Embedded Security Device – Enable** (**Dispositivo de seguridad integrada, activado**). Pulse **F10**.
16. Utilice la tecla de flecha izquierda o derecha para acceder a **File** (**Archivo**) Utilice la tecla de flecha arriba o abajo para acceder a **Save Changes and Exit** (**Guardar cambios y Salir**). Pulse **Intro** y, a continuación, pulse **F10** para confirmar.
17. Cuando se inicie Windows:

    Si utiliza Windows XP Professional o Home Edition, haga clic en **Inicio > Todos los programas > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard** (**Herramientas de seguridad integrada ProtectTools de HP > Asistente para la inicialización de seguridad integrada**).

Si utiliza Windows 2000, haga clic en **Inicio > Programas > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard** (**Herramientas de seguridad integrada ProtectTools de HP > Asistente para la inicialización de seguridad integrada**).

18. Haga clic en **Siguiente**.
19. Escriba y confirme una contraseña de Asignación de propiedad. Haga clic en **Siguiente**.

Preste atención al escribir la contraseña puesto que, por motivos de seguridad, los caracteres que se escriben no aparecen en la pantalla.

20. Asegúrese de que la opción Create a new recovery archive (Crear un nuevo archivo de recuperación) está seleccionada. En **Recovery archive location** (**Ubicación de archivo de recuperación**), haga clic en **Examinar**.
21. No acepte el nombre de archivo predeterminado. Escribe uno nuevo para evitar sobrescribir el archivo original.
22. Haga clic en **Save** (**Guardar**) y, a continuación, haga clic en **Siguiente**.
23. Escriba y confirme la contraseña de Token de recuperación de emergencia y, a continuación, haga clic en **Siguiente**.
24. Inserte un disquete para guardar la clave de Token de recuperación de emergencia. Haga clic en **Examinar** y seleccione el disquete.
25. No acepte el nombre de clave predeterminado. Escriba uno nuevo para evitar sobrescribir la clave original.
26. Haga clic en **Save** (**Guardar**) y, a continuación, haga clic en **Siguiente**.
27. Haga clic en **Siguiente** para confirmar los valores antes de iniciar la plataforma de seguridad.

Es posible que aparezca un mensaje que diga “Basic User Key cannot be loaded” (No es posible cargar la clave de usuario básico). No haga clic en el mensaje. Esto se tratará más adelante en el procedimiento y el mensaje se cerrará al cabo de unos segundos.

28. Haga clic en **Siguiente** para omitir la configuración de políticas locales.
29. Haga clic para anular la selección de la casilla de verificación **Start Embedded Security User Initialization Wizard** (**Iniciar el Asistente para la inicialización del usuario de seguridad integrada**). Haga clic en **Terminar**.
30. Haga clic con el botón derecho del ratón en el icono de ProtectTools de la barra de herramientas y haga clic en **Initialize Embedded Security restoration** (**Iniciar restauración de seguridad integrada**).

    Esto iniciará el Asistente para la inicialización de seguridad integrada ProtectTools de HP.
31. Haga clic en **Siguiente**.
32. Inserte el disquete en el que se guardó la Clave de Token de recuperación de emergencia original. Haga clic en **Examinar** y, a continuación, localice y haga doble clic en el token para introducir el nombre en el campo. El predeterminado es A:\SPEmRecToken.xml.
33. Escriba la contraseña de Token original y haga clic en **Siguiente**.
34. Haga clic en **Examinar** y, a continuación, localice y haga doble clic en el archivo de recuperación original para introducir el nombre en el campo. El predeterminado es C:\Documentos y configuración\Todos los usuarios\Datos de programa\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
35. Haga clic en **Siguiente**.
36. Haga clic en la máquina que se va a restaurar y haga clic en **Siguiente**.
37. Haga clic en **Siguiente** para confirmar los valores.
38. Si el asistente anuncia que la plataforma de seguridad se ha restaurado, continúe en el paso 39.

    Si el asistente anuncia que la restauración ha fallado, regrese al paso 10. Con cuidado, compruebe las contraseñas, la ubicación y nombre de token, y la ubicación y nombre de archivo.
39. Haga clic en Terminar.

40. Si utiliza Windows XP Professional o Home Edition, haga clic en **Inicio > Todos los programas > HP ProtectTools Embedded Security Tools > User Initialization Wizard** (**Herramientas de seguridad integrada ProtectTools de HP > Asistente para la inicialización de usuario**).

    Si utiliza Windows 2000, haga clic en **Inicio** > **Programas > HP ProtectTools Embedded Security Tools > User Initialization Wizard** (**Herramientas de seguridad integrada ProtectTools de HP > Asistente para la inicialización de usuario**).

41. Haga clic en **Siguiente**.
42. Haga clic en **Recover your basic user key** (**Recuperar la clave de usuario básico**) y luego en **Siguiente**.
43. Seleccione un usuario, escriba la contraseña de Clave de usuario básico original de ese usuario, y haga clic en **Siguiente**.
44. Haga clic en **Siguiente** para confirmar los valores y aceptar la ubicación de los datos de recuperación predeterminados.

Los pasos 45 a 49 vuelven a instalar la configuración de usuario básico original.

45. Seleccione las funciones de seguridad apropiadas y haga clic en **Siguiente**.
46. Haga clic en el cliente de correo electrónico correspondiente para seleccionarlo y, a continuación, haga clic en **Siguiente**.
47. Haga clic en el Certificado de codificación y luego en **Siguiente** para aplicarlo.
48. Haga clic en **Siguiente** para confirmar los valores.
49. Haga clic en **Terminar**.
50. Reinicie el equipo.

PRECAUCIÓN: proteja la contraseña de usuario básico. **No se puede acceder ni recuperar los datos codificados sin esta contraseña**.

DriveLock o Bloqueo de la unidad

El bloqueo de la unidad es una característica de seguridad estándar de la industria que impide el acceso no autorizado a los datos de las unidades de disco duro de compartimiento multiuso. Esta función se ha implementado como una extensión de Computer Setup. Sólo está disponible cuando se detectan unidades de disco duro compatibles con la función de bloqueo de la unidad.

La función de bloqueo de la unidad está destinada a los clientes de HP cuya preocupación principal es la seguridad de los datos. Para dichos clientes, el coste de la unidad de disco duro y la pérdida de los datos almacenados en ésta es irrelevante en comparación con los daños que pueden resultar del acceso no autorizado al contenido. A fin de equilibrar este nivel de seguridad con la necesidad práctica de facilitar una contraseña olvidada, la implementación de HP del bloqueo de la unidad utiliza un esquema de seguridad de dos contraseñas. El administrador del sistema establece y utiliza una de las contraseñas, mientras que la otra, la establece y utiliza normalmente el usuario final. La unidad no puede desbloquearse si se han perdido ambas contraseñas. Por lo tanto, la forma más segura de utilizar el bloqueo de la unidad es replicar los datos de la unidad de disco duro en un sistema de información corporativo o hacer una copia de seguridad periódicamente.

En el caso de que se perdieran ambas contraseñas de bloqueo, la unidad de disco duro quedaría inutilizada. Para los usuarios que no se ajustan al perfil de cliente anteriormente definido, esto puede suponer un riesgo inaceptable. Para los usuarios que se ajustan al perfil del cliente, puede existir un riesgo tolerable dada la naturaleza de los datos almacenados en la unidad de disco duro.

Utilización de la opción de bloqueo de la unidad

La opción DriveLock (bloqueo de la unidad) aparece en el menú Security (Seguridad) de Computer Setup. El usuario tiene la posibilidad de establecer la contraseña maestra o de activar el bloqueo de la unidad. Debe proporcionarse una contraseña de usuario para activar el bloqueo de la unidad. Dado que la configuración inicial del bloqueo de la unidad la realiza normalmente un administrador del sistema, primero debe establecerse una contraseña maestra. HP recomienda a los administradores de sistemas que establezcan una contraseña maestra tanto si desean activar el bloqueo de la unidad como si lo dejan desactivado. De esta manera, el administrador tiene la posibilidad de modificar los valores de bloqueo de la unidad en el caso de que posteriormente se active esta función. Una vez establecida la contraseña maestra, el administrador del sistema puede activar el bloqueo de la unidad o dejarlo desactivado.

En el caso de una unidad de disco duro bloqueada, la POST solicitará una contraseña para desbloquear el dispositivo. Si se ha establecido una contraseña de arranque que coincide con la contraseña de usuario del dispositivo, la POST no solicitará que se vuelva a introducir la contraseña. De lo contrario, el usuario deberá introducir una contraseña de bloqueo de la unidad. Puede utilizarse tanto la contraseña maestra como la contraseña de usuario. Los usuarios dispondrán de dos intentos para introducir una contraseña correcta. Si ninguno tiene éxito, la POST continuará pero no se podrá acceder a la unidad.

Aplicaciones de bloqueo de la unidad

La utilización más práctica de la característica de seguridad de bloqueo de la unidad es en un entorno corporativo en el que un administrador del sistema proporciona unidades de disco duro para compartimiento multiuso a los usuarios para que las utilicen en determinados equipos. El administrador del sistema será el responsable de configurar la unidad de disco duro para el compartimiento multiuso que implicará, entre otras cosas, establecer la contraseña maestra del bloqueo de la unidad. En el caso de que el usuario olvide su contraseña o que otro empleado utilice el equipo, siempre puede utilizarse la contraseña maestra para volver a establecer la contraseña de usuario y tener nuevamente acceso a la unidad de disco duro.

HP recomienda a los administradores de sistemas corporativos que optan por activar el bloqueo de la unidad que establezcan también una política corporativa para establecer y mantener las contraseñas maestras. Esto debe realizarse para evitar una situación en que un empleado modifique de forma intencionada o no ambas contraseñas de bloqueo de la unidad antes de abandonar la compañía. En tal caso, la unidad de disco duro quedaría inutilizada y debería reemplazarse. Asimismo, si no se establece una contraseña maestra, los administradores del sistema pueden encontrarse con el acceso bloqueado a una unidad de disco duro, sin posibilidad de realizar comprobaciones de rutina para detectar software no autorizado, ni otras funciones de control de activos y soporte técnico.

Para los usuarios con requisitos de seguridad menos estrictos, HP no recomienda que se active el bloqueo de la unidad. Entre los usuarios de esta categoría se incluyen los usuarios particulares o los usuarios que no mantienen datos confidenciales en las unidades de disco duro de forma habitual. Para estos usuarios, la pérdida potencial de una unidad de disco duro consecuencia del olvido de ambas contraseñas es más importante que el valor de los datos para los que se ha diseñado la función de bloqueo de la unidad. Puede restringirse el acceso a Computer Setup y DriveLock mediante la contraseña de configuración. Al especificar una contraseña de configuración y no proporcionarla a los usuarios finales, los administradores del sistema restringen los usuarios que pueden activar el bloqueo de la unidad.

Sensor de Smart Cover

El sensor de Smart Cover, disponible en determinados modelos, es una combinación de tecnología de hardware y de software que permite alertar al usuario en el caso de que se extraiga la cubierta o el panel lateral del equipo. Existen tres niveles de protección, según se describen en la tabla siguiente.

Niveles de protección del sensor de Smart Cover

Nivel	Valor	Descripción
Nivel 0	Disabled (Desactivado)	Sensor de Smart Cover desactivado (valor predeterminado).
Nivel 1	Notify User (Notificar al usuario)	Cuando se reinicia el equipo, la pantalla visualiza un mensaje en el que se indica que se ha extraído la cubierta o el panel lateral del equipo.
Nivel 2	Setup Password (Contraseña de configuración)	Cuando se reinicia el equipo, la pantalla visualiza un mensaje en el que se indica que se ha extraído la cubierta o el panel lateral del equipo. Debe introducir la contraseña de configuración para poder continuar.

✎ Estos valores pueden modificarse mediante Computer Setup. Para obtener más información sobre Computer Setup, consulte la publicación *Guía sobre la utilidad Computer Setup (F10)*.

Configuración del nivel de protección del sensor de Smart Cover

Para establecer el nivel de protección del sensor de Smart Cover, siga estos pasos:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde. Pulse **Intro** para omitir la pantalla de título, si procede.

✎ Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

3. Seleccione **Security** (**Seguridad**), a continuación, **Smart Cover** (**Cubierta inteligente**), y siga las instrucciones que aparecen en la pantalla.
4. Antes de salir, haga clic en **File > Save Changes** and **Exit** (**Archivo > Guardar cambios** y **Salir**).

Bloqueo de Smart Cover

El bloqueo de Smart Cover es un bloqueo de la cubierta controlable por software incorporado en determinados equipos de HP. Este bloqueo impide el acceso no autorizado a los componentes internos. Los equipos se entregan con la función de bloqueo de Smart Cover en la posición de desbloqueo.

PRECAUCIÓN: para garantizar una seguridad máxima del bloqueo de la cubierta, asegúrese de establecer una contraseña de configuración. La contraseña de configuración impide el acceso no autorizado a la utilidad Computer Setup.

El bloqueo de Smart Cover está disponible como opción en determinados sistemas.

Activación del bloqueo de Smart Cover

Para activar el bloqueo de Smart Cover, siga los pasos siguientes:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde. Pulse **Intro** para omitir la pantalla de título, si procede.

Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

3. Seleccione **Security** (**Seguridad**) y, a continuación, seleccione **Smart Cover** (**Cubierta inteligente**) y la opción **Locked** (**Bloqueado**).
4. Antes de salir, haga clic en **File > Save Changes** and **Exit** (**Archivo > Guardar cambios** y **Salir**).

Desactivación del bloqueo de Smart Cover

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde. Pulse **Intro** para omitir la pantalla de título, si procede.

Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

3. Seleccione **Security > Smart Cover > Unlocked** (**Seguridad > Cubierta inteligente > Desbloqueado**).
4. Antes de salir, haga clic en **File > Save Changes** and **Exit** (**Archivo > Guardar cambios** y **Salir**).

Utilización de la llave de seguridad de Smart Cover

Si activa el bloqueo Smart Cover y no puede escribir la contraseña para desactivar el bloqueo, necesitará la llave de seguridad de Smart Cover para abrir la cubierta del equipo. Necesitará la llave en cualquiera de las circunstancias siguientes:

- Corte de alimentación
- Fallo de arranque
- Fallo de un componente de PC (por ejemplo, procesador o fuente de alimentación)
- Olvido de la contraseña

PRECAUCIÓN: la llave de seguridad de Smart Cover es una herramienta especializada de HP. Sea previsor y solicite esta llave antes de necesitarla al proveedor o servicio técnico autorizado.

Para obtener la llave de seguridad, siga uno de los pasos siguientes:

- Póngase en contacto con el servicio técnico autorizado de HP.
- Llame al número correspondiente que se indica en la garantía.

Para obtener más información sobre cómo utilizar la llave de seguridad de Smart Cover, consulte la publicación *Guía de referencia del hardware*.

Seguridad del registro de arranque maestro

El registro de arranque maestro contiene información necesaria para arrancar correctamente un disco y acceder a los datos almacenados en el mismo. La seguridad del registro de arranque maestro puede impedir cambios inadvertidos o maliciosos en el registro de arranque maestro, tales como los provocados por ciertos virus informáticos o por el uso incorrecto de determinadas utilidades de disco. También permite recuperar el último registro de arranque maestro correcto, si se detectan cambios en dicho registro cuando se reinicia el sistema.

Para activar la seguridad del registro de arranque maestro, siga estos pasos:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde. Pulse **Intro** para omitir la pantalla de título, si procede.

Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

3. Seleccione **Security > Master Boot Record Security > Enabled** (**Seguridad > Seguridad del registro de arranque maestro > Activado**).
4. Seleccione **Security > Save Master Boot Record** (**Seguridad > Guardar registro de arranque maestro**).
5. Antes de salir, haga clic en **File > Save Changes** and **Exit** (**Archivo > Guardar cambios** y **Salir**).

Si se ha activado la seguridad del registro de arranque maestro, el BIOS impide que se efectúen cambios en el registro de arranque maestro del disco de arranque actual cuando se trabaja en el modo de seguridad de MS-DOS o Windows.

La mayoría de los sistemas operativos controlan el acceso al registro de arranque maestro del disco de arranque actual; el BIOS no puede impedir que se efectúen cambios cuando se está ejecutando el sistema operativo.

Cada vez que se enciende o se reinicia el equipo, el BIOS compara el registro de arranque maestro del disco de arranque actual con el registro anteriormente guardado. Si se detectan cambios o si el disco de arranque actual es el disco cuyo registro de arranque maestro se guardó anteriormente, aparecerá un mensaje parecido al siguiente:

1999: se ha modificado el registro maestro de arranque

Pulse cualquier tecla para acceder a la utilidad de configuración y configurar la seguridad del registro de arranque maestro.

Tras acceder a Computer Setup, debe:

- Guardar el registro de arranque maestro del disco de arranque actual
- Restaurar el registro de arranque maestro guardado anteriormente, o bien
- Desactivar la característica de seguridad del registro de arranque maestro.

Debe conocer la contraseña de configuración, en el caso de que exista alguna.

Si se detectan cambios o si el disco de arranque actual **no** es el disco cuyo registro de arranque maestro se guardó anteriormente, aparecerá un mensaje parecido al siguiente:

2000: se ha modificado el registro maestro de arranque de la unidad de disco duro

Pulse cualquier tecla para acceder a la utilidad de configuración y configurar la seguridad del registro de arranque maestro.

Tras acceder a Computer Setup, debe:

- Guardar el registro de arranque maestro del disco de arranque actual o bien
- Desactivar la característica de seguridad del registro de arranque maestro.

Debe conocer la contraseña de configuración, en el caso de que exista alguna.

En el caso improbable de que el registro de arranque maestro guardado previamente esté dañado, aparecerá un mensaje parecido al siguiente:

1998: se ha perdido el registro maestro de arranque

Pulse cualquier tecla para acceder a la utilidad de configuración y configurar la seguridad del registro de arranque maestro.

Tras acceder a Computer Setup, debe:

- Guardar el registro de arranque maestro del disco de arranque actual o bien
- Desactivar la característica de seguridad del registro de arranque maestro.

Debe conocer la contraseña de configuración, en el caso de que exista alguna.

Antes de crear una partición del disco de arranque actual o formatearlo

Asegúrese de que se ha desactivado la seguridad del registro de arranque maestro antes de modificar las particiones del disco de arranque actual o dar formato a dicho disco. Algunas utilidades de disco, tales como FDISK y FORMAT, intentan actualizar el registro de arranque maestro. Si la seguridad del registro de arranque maestro está activada cuando modifique la partición o el formato del disco, recibirá mensajes de error de la utilidad de disco o una advertencia de la seguridad del registro de arranque maestro la próxima vez que encienda o reinicie el equipo. Para desactivar la seguridad del registro de arranque maestro, siga estos pasos:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar el sistema > Reiniciar el equipo**.
2. Pulse la tecla **F10** tan pronto como la luz del monitor se ponga en verde. Pulse **Intro** para omitir la pantalla de título, si procede.

Si no pulsa la tecla **F10** en el momento adecuado, tendrá que apagar el equipo, volverlo a encender y pulsar otra vez la tecla **F10** para acceder a la utilidad.

3. Seleccione **Security > Master Boot Record Security > Disabled** (**Seguridad > Seguridad del registro de arranque maestro > Desactivado**).
4. Antes de salir, haga clic en **File > Save Changes** and **Exit** (**Archivo > Guardar cambios** y **Salir**).

Candado con cadena

En el panel posterior del equipo hay un candado con cadena para sujetar físicamente el equipo al área de trabajo.

Para obtener instrucciones ilustradas, consulte la publicación *Guía de referencia del hardware* que se encuentra en el CD *Biblioteca de documentación*.

Tecnología de identificación de huellas digitales

Al eliminar la necesidad de introducir contraseñas de usuario, la tecnología de identificación de huellas digitales de HP refuerza la seguridad de la red, simplifica el proceso de conexión y reduce los costes asociados con la gestión de redes corporativas. Esta tecnología, cuyo precio es razonable, ya no está dirigida solamente a organizaciones de alta tecnología y seguridad.

La compatibilidad con la tecnología de identificación de huellas digitales varía según el modelo.

Para obtener más información, visite:

http://h18000.www1.hp.com/solutions/security.

Recuperación y notificación de fallos

Las funciones de recuperación y notificación de fallos combinan tecnología de hardware y de software innovadora para impedir la pérdida de datos críticos y minimizar los periodos de no disponibilidad no planeados.

Cuando se produce un fallo, el equipo visualiza un mensaje de alerta local que contiene una descripción del fallo y las acciones recomendadas. Posteriormente, puede verificar el funcionamiento del sistema actual mediante la utilización de HP Client Manager. Si el equipo está conectado a una red gestionada por HP Insight Manager, HP Client Manager u otra aplicación de administración de sistemas, también enviará un aviso de fallo a la aplicación de gestión de red.

Sistema de protección de unidades

El sistema de protección de unidades (DPS del inglés Drive Protection System) es una herramienta de diagnóstico incorporada en las unidades de disco duro que están instaladas en determinados equipos de HP. DPS está diseñado para ayudar a diagnosticar problemas que pueden requerir una sustitución de la unidad de disco duro no cubierta por la garantía.

Cuando se fabrican los equipos de HP, las unidades de disco duro instaladas se someten a prueba mediante DPS y se graba un registro permanente de información clave en la unidad. Cada vez que se ejecuta DPS, los resultados de la prueba se graban en la unidad de disco duro. El servicio técnico puede utilizar esta información para diagnosticar las condiciones que le han llevado a ejecutar el software DPS. Para obtener instrucciones acerca del uso del sistema de protección de unidades, consulte la *Guía de solución de problemas*.

Fuente de alimentación con protector de sobretensión

Una fuente de alimentación con protector de sobretensión integrada proporciona mayor fiabilidad cuando el equipo se ve afectado por una sobretensión imprevista de la corriente. Esta fuente de alimentación está diseñada para resistir sobretensiones de hasta 2.000 voltios sin causar periodos de no disponibilidad ni pérdidas de datos en el equipo.

Sensor térmico

El sensor térmico es una función de hardware y de software que controla la temperatura interna del equipo. Esta función muestra un mensaje de advertencia cuando se sobrepasa el rango normal de temperaturas, lo que proporciona tiempo al usuario para emprender una acción antes de que se produzcan daños en los componentes internos o pérdidas de datos.

Índice